REMARKS

Applicants and Applicants' attorney express appreciation to the Examiner for the courtesies extended during the recent Interview conducted on June 14, 2004. The claim amendments made by this paper are consistent with the proposed claim amendments and corresponding arguments discussed during the Interview.

Claims 1-8 and 18-29 are pending, of which claim 1 is an independent method claim drafted from the perspective of a server computer system, claim 8 is an independent computer program product claim corresponding to independent method claim 1, claim 18 is an independent method claim drafted from the perspective of a controlling computer system, claim 25 is an independent computer program product claim corresponding to independent method claim 18, and claim 26 is an independent claim directed to a computer readable medium storing a data structure. As indicated above, claims 1, 18, and 26 have been amended by this paper.

The Office Action rejected all claims, except claims 7 and 24, under 35 U.S.C. § 102(e) as being anticipated by "LPRng-HOWTO" authored by Powell ("*Powell*"), and rejected claims 7 and 24 under 35 U.S.C. § 103(a) as being unpatentable over *Powell* in view of U.S. Patent No. 6,446,204 to Pang et al. ("*Pang*").[1]

Applicants' invention, as claimed for example in independent method claim 1, relates to a method of authenticating a subset of a plurality of client computer systems. The method comprises a server computer system receiving a request from a controlling client computer system, the request including an instruction identifying at least one of a plurality of authentication methodologies that is to be used for authenticating the subset of client computer systems when the subset of client computer systems request service from the server computer system, the at least one of the plurality of authentication methodologies having been selected based on authentication abilities and access rights of the subset of client computer systems. The server computer system stores methodology information that identifies the at least one of the plurality of authentication methodologies and the subset of client computer systems to be authenticated with the at least one of the plurality of authentication methodologies so that an acceptable authentication methodology can be identified efficiently and without the subset of

[1]Although the prior art status of all cited art is not being challenged at this time, Applicants reserve the right to do so in the future. Accordingly, any arguments and amendments made herein should not be construed as acquiescing to any prior art status or asserted teachings of the cited art.

client computer systems unnecessarily revealing secret information. The server computer system receives a subsequent request from the subset of client computer systems for service from the server computer system, and upon receiving the subsequent request, determines how to authenticate the subset of client computer systems based on the stored methodology information, and authenticates the subset of client computer systems using the least one authentication methodology identified in the instruction. Claim 8 simply recites a computer-readable medium having computer-executable instructions for performing the acts recited in claim 1.

Applicants' invention as claimed for example in independent method claim 18 relates to controlling the type of authentication methodology used when a server computer system authenticates a subset of client computer systems. The method comprises a controlling client computer system composing a request including an instruction identifying an authentication methodology that is to be used by a server computer system for authenticating the subset of client computer systems, the authentication methodology having been selected based on authentication abilities and access rights of the subset of client computer systems. The controlling client computer system transmits the request to the server computer system, wherein the authentication methodology identified in the instruction is used by the server computer system to authenticate the subset of client computer systems when the server computer system receives one or more subsequent requests from the subset of client computer systems for service from the server computer system so that an acceptable authentication methodology can be identified efficiently and without the subset of client computer systems unnecessarily revealing secret information. Similar to claim 8, claim 25 simply recites a computer-readable medium having computer-executable instructions for performing the acts recited in claim 18.

Applicants' invention, as claimed for example in independent claim 26, relates to a computer-readable medium storing a data structure having a plurality of fields. The data structure comprises a plurality of client identifier fields that each identify a client computer system that is connected to a server computer system, and for each identified client computer system, at least one authentication field that identifies an authentication method to be used by the server computer system for authenticating the client computer system upon receiving a request from the client computer system for service, the authentication method having been selected

based on authentication abilities and access rights of the subset of client computer systems so that the subset of client computer systems need not unnecessarily reveal secret information.

For example, as Applicants note with respect to Figure 2, a "client computer system 22a may have right to perform highly sensitive operations using the server computer system 210. Therefore, it was appropriate that only reliable authentication methods be used to authenticate the client computer system." Specification, p. 18, ll. 1-3. Applicants also note that in "addition to the efficiency advantages, refraining from attempting unacceptable authentication methods has certain security advantages as well. For example, some methods of authentication including basic authentication reveal the user's password to the network. Thus, attempting basic authentication if basic authentication is not going to work would result in unnecessarily risking the revealing of the password." Specification, p. 19, ll. 14-18.

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." MPEP § 2131. That is, "for anticipation under 35 U.S.C. 102, the reference must teach every aspect of the claimed invention either explicitly or impliedly." MPEP § 706.02. Applicants also note that "[i]n determining that quantum of prior art disclosure which is necessary to declare an applicant's invention 'not novel' or 'anticipated' within section 102, the stated test is whether a reference contains an 'enabling disclosure.'" MPEP § 2121.01. In other words, a cited reference must be enabled with respect to each claim limitation.

Powell discloses a print spooler that provides privacy and authentication services for clients. See *Powell*, Section 12. In *Powell*, the client requesting a print job specifies the type of authentication to be carried out. See *Powell*, Section 12.4 and 12.5. One server may forward print jobs to another server, in which case the forwarding or sending server takes the part of the client. See *Powell*, Section 12.6.

However, among other things, *Powell* fails to teach or suggest a controlling client computer identifying an authentication methodology to be used by a server computer when authenticating a subset of client computer systems, the authentication methodology having been selected based on the authentication abilities and access rights of the subset of client computer systems so that an acceptable authentication methodology can be identified efficiently and without the subset of client computer systems unnecessarily revealing secret information.

Rather, as indicated above, in *Powell* the client requesting the print job specifies the type of authentication to be carried out.

Accordingly, Applicants respectfully submit that *Powell* fails to teach or suggest every aspect of Applicants' invention, as claimed for example in independent claims 1, 8, 18, 25, and 26, as amended. Therefore, the rejections of independent claims 1, 8, 18, 25, and 26, under 35 U.S.C. § 102(e) as being anticipated by *Powell* have been overcome and should be withdrawn. During the Interview, the Examiner seemed to concur with this position in that the Interview Summary states the proposed amendments appear to overcome the art of record, but that further consideration and/or searching will be undertaken upon receiving Applicants' formal reply.

Based on at least the foregoing reasons, Applicants respectfully submit that the cited prior art fails to anticipate or make obvious Applicants invention, as claimed for example, in independent claims 1, 8, 18, 25, and 26. Applicants note for the record that the remarks above render the remaining rejections of record for the independent and dependent claims moot, and thus addressing individual rejections or assertions with respect to the teachings of the cited art is unnecessary at the present time, but may be undertaken in the future if necessary or desirable, and Applicants reserve the right to do so.

In the event that the Examiner finds any remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney.

Dated this 21st day of July, 2004.

Respectfully submitted,

RICK D. NYDEGGER
Registration No. 28,651
ERIC M. KAMERATH
Registration No. 46,081
Attorneys for Applicant

Customer No. 022913

RDN:EMK:cm
CM0000003902V001